

REMARKS

Claims 1-15 remain pending.

At page 2 of the Office Action, new application papers are requested with lines double spaced on good quality paper. In response, Applicants submit herewith a substitute specification with lines double spaced on good quality paper and in compliance with 37 C.F.R. §§ 1.125 (b) and (c). This request necessitates that Applicants submit the substitute specification. No new matter is added by or in the substitute specification.

CLAIM REJECTION UNDER 35 USC §102

At page 3 of this Office Action, claims 8-11 are rejected under 35 U.S.C § 102(e) as being anticipated by U.S. Patent No. 6, 584, 566 to Hardjono. Applicants submit that claims 8-11 are not anticipated by Hardjono because Hardjono does not disclose all of the elements of Applicants' invention.

Hardjono teaches distributed group key management for multicast security in a computer network having a collection of security domains based on computer systems (Col. 3, line 61 – Col. 4, line 19). An initiator key server distributes a first key set to a plurality of key servers. The first key set includes an initial common group key (e.g., CGK:I) and a replacement CGK (e.g., CGK:R). The initial CGK, but not the replacement CGK, is initially distributed, as a current CGK for multicast messages, to clients of the key servers that are currently members of a multicast group (Col. 4, lines 63-66). When re-keying of the current CGK of the multicast group is needed, each of the key servers subsequently distributes to their respective clients, that

are currently members of the multicast group, the replacement CGK, previously distributed to the key servers, as the current CGK (Col. 5, lines 2-10). Hardjono additionally teaches that each key server in a security domain shares a private-key (e.g., KSK) with the initiator key server (Col. 5, lines 48-55), each domain is associated with a domain key (e.g., DK) known only by the key server of the corresponding domain and members of such domain and optionally the initiator key server (Col. 5, lines 56-65), and a server group key (e.g., SGK) having a security association is shared by key servers, including the initiator key server, in a server group (Col. 6, lines 25-42). In essence, Hardjono teaches to use a variety of "group" specific keys for distributing a pair of common group keys, namely an initial CGK and a replacement CGK that is swapped out for the initial CGK when re-keying is desired.

In one embodiment, Applicants' invention is directed to operating a key management center to excise a compromised node using a key encryption key (KEK) hierarchy (see generally FIG. 2 and Applicants' original Specification at page 7, lines 16-22) having tier-group specific KEKs to encrypt a new traffic encryption key (TEK). For a system having "n" tiers where each group corresponds to "y" groups of the next lower tier, the entire network can be re-keyed with  $(n+1)(y-1)$  messages (see Applicants' original Specification at page 8, lines 7-16) demonstrating the efficiency of Applicants' invention. Claim 8 recites the step of "from a list of top tier key encryption keys, selecting a top tier key encryption key that does not correspond to a group that includes the compromised node [emphasis added]". Applicants submit that Hardjono does not teach the top tier key encryption key selection step recited in claim 8.

In contrast with the Applicants' invention, Hardjono takes an entirely different approach to re-keying encryption keys. The keys taught by Hardjono represent a variety keys used to

communicate between and among the key servers and the members (see FIG. 1). DK is used by a key server to communicate with all members in the domain while MK is used for individual communication between the key server and a specific member. SGK is used for communication among all of the key servers while KSK is used for communication between the initiator key server and a specific key server. Hardjono does not mention "tiers" of key encryption keys.

Identifying a top tier key encryption key in Hardjono is vague if not contrary to Applicants' step of selecting a top tier key encryption key. In the event of re-keying, Hardjono teaches two methods of notification (see Col. 8, lines 34-56). The first method taught by Hardjono uses SGK which is common to all key servers in the group. Clearly, using SGK is contrary to "selecting a top tier key encryption key that does not correspond to a group that includes the compromised node" as recited in claim 8 because no exclusion of a compromised node is made using SGK. The second method taught by Hardjono is using the private server specific KSKs. However, using KSKs also does not exclude compromised nodes. To isolate a leaving member, Hardjono teaches to use a different key that has a characteristic to make such key secure from the leaving member. For example, KSK is used in the second method because members do not have access to KSK. The use of DK by a key server as taught by Hardjono (see Col. 9, lines 1-13), is not "selecting a top tier key" as recited in claim 8 because Hardjono teaches simply that "each key server without a client membership change distributes the replacement common group key to its multicast members using its domain key." (Col. 9, lines 1-3). No top tier key is selected in Hardjono.

Additionally, it is unclear whether the domain key taught by Hardjono is a "top tier key" because although Hardjono appears to teach some relationship between key servers and

members and between domains and members, Hardjono discloses that DK is used to multicast to the whole group or provide a limited-scope multicast within the domain (see Col. 9, lines 4-9). From this, DK is not a true tier-group specific key as all "tier keys" are in Applicants' invention.

Claim 8 further recites the step of "encrypting a new traffic encryption key using the top tier key encryption key, to produce an encrypted traffic encryption key [emphasis added". Applicants submit that Hardjono does not disclose the encrypting step recited in claim 8 because Hardjono does not teach using the top tier key encryption key to encrypt a new traffic encryption key. As previously mentioned, it is unclear whether the domain key taught by Hardjono is a "tier key" as recited in claim 8, and it is further unclear whether the domain key taught by Hardjono is a "top tier key". At best, Hardjono discloses that DK may be used to multicast to a whole group or multicast in a limited-scope which prescribes DK in a manner inconsistent with the term "top tier key" as recited in claim 8.

Applicants' respectfully submit that claim 8 is patentably distinguished from Hardjono because Hardjono does not teach the top tier selecting step nor the encrypting step recited in claim 8. Because of the foregoing discussion regarding the patentability of claim 8 and because claims 9-11 depend from claim 8, Applicants respectfully submit that claims 9-11 are likewise patentably distinguished from Hardjono.

At page 3 of this Office Action, claims 12-15 are rejected under 35 U.S.C § 102(e) as being anticipated by U.S. Patent No. 5,592,552 to Fiat. Applicants submit that Fiat does not disclose all of the elements of Applicants' invention.

Fiat discloses selective broadcasting methods to transmit message data signals to a plurality of subscriber subsets within a set of subscribers based on memory per user/subscriber and transmission length of messages as related to stored keys for each user. One method is to define partitions in a population of subscribers where each partition has subscriber sets (see Col. 12, lines 59-65). Each partition and each subscriber set within the respective partition set is provided a unique one-resilient scheme, and key(s) are distributed by the scheme (see Col. 12, line 66 – Col. 13, line 10). Fiat does not teach or suggest a key management center as in Applicants' invention.

One embodiment of Applicants' invention is a key management center (KMC) that includes a data structure occupying a portion of KEK hierarchy storage within the memory of the KMC (see Applicants' original Specification at page 9, lines 1-6). Each data structure member includes a plurality of tier-group specific KEKs. In one data structure member, each of the KEKs corresponds to a node in a communications system, and in progressive data structure members, each respective tier-group specific KEK corresponds to a prior group of tier-group specific KEKs for the prior data structure member (see Applicants' original Specification at page 9, lines 7-15). Applicants submit that Fiat does not disclose a key management center having a storage device as recited in claim 12.

Claim 12 recites as an element "a storage device coupled to the encryption device, the storage device being configured to hold a hierarchy of key encryption keys [emphasis added]." Although Fiat discloses a system having n subscriber memories storing a set of keys (see Fiat, claims 17-20), Fiat does not teach or suggest a hierarchy of key encryption keys. Disclosure of a partitioning scheme for a population of subscribers by Fiat (see Col. 12, line 58 – Col. 13, line

10) is in the context of key or multiple keys distribution to the subscribers. At best, Fiat teaches that a different number of keys are stored in different subscriber memories based on subscriber population. Fiat simply does not teach a hierarchy of key encryption keys nor a storage device configured to hold the same.

Applicants' respectfully submit that claim 12 is patentably distinguished from Fiat because Fiat does not teach "a storage device being configured to hold a hierarchy of key encryption keys" as recited in claim 12. Because of the foregoing discussion regarding the patentability of claim 12 and because claims 13-15 depend from claim 12 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 13-15 are likewise patentably distinguished from Fiat

From the foregoing discussion, Applicants submit that rejection of claims 8-15 under 35 U.S.C § 102(e) has been overcome.

#### CLAIM REJECTION UNDER 35 USC §103

At page 2 of this Office Action, claims 1-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,584,566 to Hardjono as applied to claims 8-11 above, and further in view of U.S. Patent No. 6,195,751 to Caronni et al. Applicants submit that claims 1-7 are not obviated by Hardjono in view of Caronni et al. because none of the cited references, either alone or in combination, disclose all of the elements of Applicants' invention.

Claim 1 recites the step of "broadcasting a new traffic encryption key to each of a plurality of top tier groups in a top level tier, wherein the plurality of top tier groups excludes a group that includes the compromised node". As previously set forth hereinabove with regard to

the patentability of claims 8-15, Hardjono discloses some relationship between key servers and members and between domains and members, but Hardjono does not disclose top tier groups. Instead, Hardjono discloses that the pair of CGKs is initially distributed to all key servers (see Col. 4, lines 63-66), and the initial CGK is subsequently distributed to clients of the key servers that are members (see Col. 5, lines 24-31). In response to re-key needs, Hardjono discloses that the initiator key server multicasts a new initial and replacement CGK (Col. 8, lines 57-60). Hardjono also discloses that the replacement CGK is distributed to the clients of the key servers that are members (see Col. 5, lines 37-46). However, Hardjono does not teach or suggest distributing the replacement CGK to each of the key servers excluding the key server having the compromised node. In contrast, Hardjono teaches to multicast to all key servers a new initial and replacement CGK. Likewise, Caronni et al. do not disclose the broadcasting step recited in claim 1.

Caronni et al. disclose a system for secure multicast using a first key that is shared with all participant entities and a set of second keys that is shared with a subset of the participant entities. It is important to note that Caronni et al. also teach that a group key management component uses the first key and a number of the second keys. This group key management component stores and maintains the first and second keys in a group key database that is in a non-hierarchical, flat fashion (see Col. 4, lines 41-51). Caronni et al. are cited in this Office Action for disclosing recursive broadcasting. Applicants submit that Caronni et al. do not teach recursive broadcasting as recited in claim 1.

Claim 1 recites the step of "within the group that includes the compromised node, recursively broadcasting the new traffic encryption key to groups of nodes at a succession of

lower tiers". In contrast, Caronni et al. discloses that during exclusion of a participant, an excluder chooses a new TEK that is encrypted with all KEKs not shared with the participant. The KEKs known to the participant are thrown out, and new KEKs are assigned. This information populates a table which is sent to the participant group. The other participants able to decrypt the new TEK supplements the table with new KEKs which it holds and rebroadcasts the table. This rebroadcasting taught by Caronni et al. has no effect on groups at successively lower tiers. Caronni et al. simply teaches broadcasting an updated table with new KEKs to other participants.

Applicants submit that it is inappropriate to combine Carroni et al. with Hardjono because Carroni et al. teach contrary to Hardjono. Carroni et al. teach that a respective participant has a TEK and one or more KEKs and independently chooses a new TEK and assigns new KEKs during re-keying (see Col. 14, lines 55-67). In contrast, Hardjono teaches that key servers multicast a new pair initial CGK and replacement CGK. Hardjono teaches an opposite method of re-keying than Carroni et al.

Furthermore, Applicants submit that the hypothetical combination of Caronni et al. with Hardjono does not result in Applicants' invention. In particular, Caronni et al. teaches the use of a non-hierarchical, flat fashion key organization which implies no tier grouping of keys. Hardjono is silent with respect to any organization of keys. Any resulting combination of Caronni et al. with Hardjono would include the flat fashion key organization which is completely contrary to Applicants' tier group hierarchy.

Applicants' respectfully submit that claim 1 is patentably distinguished from the cited references, either alone or in combination, because the cited references do not teach nor suggest



the steps recited in claim 1. Because of the foregoing discussion regarding the patentability of claim 1 and because claims 2-7 depend from claim 1 or an intermediate claim depending therefrom, Applicants respectfully submit that claims 2-7 are likewise patentably distinguished from the cited references.

From the foregoing discussion, Applicants submit that rejection of claims 1-7 under 35 U.S.C § 103(a) has been overcome.

#### PRIOR ART MADE OF RECORD AND NOT RELIED UPON

The prior art made of record and not relied upon in this Office Action has been considered by Applicants and determined not to be pertinent, particularly in light of the foregoing differences between the claimed invention and the cited references.

#### CONCLUSION

In view of Applicants' amendments and remarks, it is respectfully submitted that the rejections under 35 U.S.C. §102(e) and §103(a) have been overcome. Accordingly, Applicants respectfully submit that the application, as amended, is now in condition for allowance, and such allowance is therefore earnestly requested. Should the Examiner have any questions or wish to further discuss this application, Applicants request that the Examiner contact the Applicants' attorneys at 480-385-5060.

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for any extension necessary to prevent abandonment on this application, please consider this as a request for an extension for the

Appl. No. 09/536,577

Response dated March 30, 2004

Reply to Office Action of Jan. 22, 2004

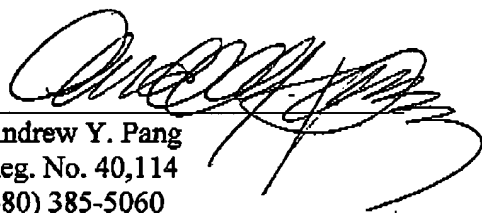
required time period and/or authorization to charge Deposit Account No. 50-2117 for any fee which may be due.

Respectfully submitted,

INGRASSIA FISHER & LORENZ, P.C.

Dated: March 30, 2004

By:

  
Andrew Y. Pang  
Reg. No. 40,114  
(480) 385-5060